Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Combinatorial Theory, Series A 101 (2003) 131–146

Journal of Combinatorial Theory Series A

http://www.elsevier.com/locate/jcta

The invariant factors of some cyclic difference sets

David B. Chandler and Qing Xiang*

Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA

Received 22 December 2001

Abstract

Using the Smith normal forms of the symmetric designs associated with the HKM and Lin difference sets, we show that not only are these two families of difference sets inequivalent, but also that the associated symmetric designs are nonisomorphic.

Keywords: Difference set; Gauss sum; Singer difference set; Stickelberger's theorem; Teichmüller character

1. Introduction

We assume that the reader is familiar with the basic theory of difference sets as can be found in [4,12].

One of the most important classes of difference sets is the family of difference sets with parameters

$$v = \frac{q^m - 1}{q - 1}, \qquad k = \frac{q^{m-1} - 1}{q - 1}, \qquad \lambda = \frac{q^{m-2} - 1}{q - 1}, \tag{1.1}$$

where q is a prime power, and m is a positive integer greater than 2. In this note, difference sets with parameters (1.1), or the complementary parameters $v = (q^m - 1)/(q - 1)$, $k = q^{m-1}$, $\lambda = q^{m-2}(q - 1)$ are called difference sets with *classical* parameters. These difference sets exist in abundance when m is composite, see [20] for a survey of known constructions up to 1999.

*Corresponding author.

E-mail addresses: chandler@math.udel.edu (D.B. Chandler), xiang@math.udel.edu (Q. Xiang).

0097-3165/03/$ - see front matter
doi:10.1016/S0097-3165(02)00023-7

In the study of difference sets with classical parameters, one often faces the following question. After constructing a family of difference sets with classical parameters, how can one tell whether the difference sets constructed are equivalent to the known ones or not? This question was usually answered by comparison of p-ranks of the difference sets involved, see [2,6,7]. Recent advances in constructions of difference sets with classical parameters have provided us with examples of $(\frac{3^m-1}{2}, 3^{m-1}, 2\cdot 3^{m-2})$ difference sets having the same 3-ranks, but it remained to decide whether these difference sets are equivalent or not. These examples are the HKM difference sets and the Lin difference sets. The purpose of this note is to demonstrate that we do have tools beyond p-ranks to deal with inequivalence problems of difference sets. Using the Smith normal forms of the designs associated with the HKM and Lin difference sets, we will show that not only are the HKM and Lin difference sets inequivalent, but also that the associated designs are nonisomorphic.

We now give the definitions of the HKM and Lin difference sets. We will use standard notation: $\mathbb{F}_{q^m}$ denotes the finite field with q^m elements, $\mathbb{F}_{q^m}^*$ is the multiplicative group of $\mathbb{F}_{q^m}$, $\mathrm{Tr}_{q^m/q}$ denotes the trace from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, and the map $\rho : \mathbb{F}_{q^m}^* \to \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ denotes the natural epimorphism.

Definition 1.1. Let $q = 3^e$, $e \geqslant 1$, let $m = 3k$, k a positive integer, $d = q^{2k} - q^k + 1$, and set

$$R = \{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{q^m/q}(x + x^d) = 1\}. \tag{1.2}$$

Then $\rho(R)$ is a $((q^m-1)/(q-1), q^{m-1}, q^{m-2}(q-1))$ difference set in $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$. This is proved by using the language of sequences with ideal 2-level autocorrelation in [8] in the case $q = 3$. See [6] for a complete proof of this fact (the paper [6] also showed that R is a relative difference set). We will call this difference set $\rho(R)$ the HKM difference set.

Definition 1.2. Let $m \geqslant 3$ be an odd integer, let $d = 2\cdot 3^{(m-1)/2} + 1$, and set

$$R = \{x \in \mathbb{F}_{3^m} \mid \mathrm{Tr}_{3^m/3}(x + x^d) = 1\}. \tag{1.3}$$

Then $\rho(R)$ is a $((3^m-1)/2, 3^{m-1}, 2\cdot 3^{m-2})$ difference set in $\mathbb{F}_{3^m}^*/\mathbb{F}_3^*$. This was conjectured by Lin, and recently proved by Arasu et al. [1]. We will call this difference set $\rho(R)$ the Lin difference set.

In the case $q = 3$, $m = 3k$, $k > 1$, the 3-rank of the HKM difference set is $2m^2 - 2m$. This was shown in [6,16]. One can similarly show that the Lin difference set has 3-rank $2m^2 - 2m$, where $m > 3$ is odd, see [16]. Therefore when m is an odd multiple of 3, these two difference sets have the same 3-rank. It is therefore natural to ask whether there are some other invariants beyond 3-rank which can be used to distinguish these two families of difference sets. We will answer this question in the affirmative by using Smith normal forms of the incidence matrices of the symmetric designs developed from these difference sets. We mention in passing that the Smith

normal form of the incidence matrix between the points and the lines of $\mathrm{PG}(2,p^s)$ was determined by Lander [11], Black and List [5] determined the Smith normal forms of the Singer designs when the ground field is a prime field. More recently, Liebler and Sin [14], each determined the Smith normal form of the incidence matrix between the points and hyperplanes of $\mathrm{PG}(m,p^s)$. Also Sin [19] computed the invariant factors of the incidence matrices between points and subspaces of any fixed dimension in $\mathrm{PG}(m,p)$.

2. The Smith normal forms of difference sets

Let G be a (multiplicative) abelian group of order v, and let D be a (v,k,λ) difference set in G. Then $\mathscr{D}=(\mathscr{P},\mathscr{B})$ is a (v,k,λ) symmetric design with a regular automorphism group G, where the set $\mathscr{P}$ of *points* of $\mathscr{D}$ is G, and where the set $\mathscr{B}$ of *blocks* of $\mathscr{D}$ is $\{Dg \mid g\in G\}$. This design is usually called the *development* of D. The *incidence matrix of* $\mathscr{D}$ is the v by v matrix A whose rows are indexed by the blocks B of $\mathscr{D}$ and whose columns are indexed by the points g of $\mathscr{D}$, where the entry $A_{B,g}$ in row B and column g is 1 if $g\in B$, and 0 otherwise.

Since A is an integral matrix, we know from linear algebra that there exist two integral unimodular matrices P and Q such that

$$PAQ=\mathrm{diag}(d_1,d_2,\ldots,d_v), \tag{2.1}$$

where d_i are integers, and $d_i|d_{i+1}$, for $i=1,2,\ldots,v-1$. Moreover, the d_i are determined up to sign and are called *the invariant factors* of A. The diagonal matrix $\mathrm{diag}(d_1,d_2,\ldots,d_v)$ is called *the Smith normal form* of A. For convenience, we define *the Smith normal form of the symmetric design* $\mathscr{D}$ to be the Smith normal form of its incidence matrix A. This Smith normal form is also called *the Smith normal form of the difference set* D, and the invariant factors of A are called *the invariant factors* of D.

Let $\mathscr{D}_1$ and $\mathscr{D}_2$ be two (v,k,λ) symmetric designs, and let A_1 and A_2 be the incidence matrices of $\mathscr{D}_1$ and $\mathscr{D}_2$, respectively. If $\mathscr{D}_1$ and $\mathscr{D}_2$ are isomorphic, that is, there exist two permutation matrices U and V such that

$$UA_1V=A_2, \tag{2.2}$$

then it is clear that A_1 and A_2 should have the same Smith normal form. So the Smith normal forms can help us decide whether two symmetric designs are isomorphic or not.

If the design $\mathscr{D}$ is developed from a (v,k,λ) abelian difference set, then the following lemmas can be used to compute the number of invariant factors not divisible by p^α, where p is a prime not dividing v.

We will start with the local case, then move to the global case. The following notation will be used: p is a prime, v_p is the p-adic valuation on $\mathbb{Q}$, $\mathbb{Q}_p$ is the field of p-adic rational numbers (the completion of $\mathbb{Q}$ with respect to v_p), $\mathbb{Z}_p$ is the ring of p-adic integers, ζ_v a primitive vth root of unity in the algebraic closure of $\mathbb{Q}_p$,

$K = \mathbb{Q}_p(\zeta_v)$, $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}_p$ in K, and finally $\mathfrak{p}$ is the unique maximal ideal in $\mathcal{O}_K$ lying above p.

Lemma 2.1. *Let G be an abelian group of order v, and p be a prime not dividing v. Let D be a (v,k,λ) difference set in G, and let α be a positive integer. Then the number of invariant factors of D which are not divisible by p^α is equal to the number of characters $\chi : G \to K$ satisfying*

$$\chi(D) \not\equiv 0 \pmod{\mathfrak{p}^\alpha}. \tag{2.3}$$

Proof. Let $\sum_{g\in G} a_g g$, where $a_g = 0$ or 1, be the group ring element in $\mathbb{Z}[G]$ corresponding to the subset D of G, that is, $a_g = 1$ if $g \in D$, 0 otherwise. We associate with D the matrix $A = (a_{g^{-1}h})$ whose rows and columns are indexed by the group elements g and h. This matrix A can serve as the incidence matrix of the design $(G, \{Dg \mid g \in G\})$ developed from D.

Let $(\chi^{-1}(g))$ be a matrix whose rows are labeled by the v characters $\chi : G \to K$ and whose columns are labeled by the v group elements g, so that the entry in row χ and column g is $\chi^{-1}(g)$. This matrix, considered as a matrix with entries in $\mathcal{O}_K$, is nonsingular since $\gcd(p,v) = 1$ and $\frac{1}{v}(\chi^{-1}(g))(\chi(g))^\top$ is the identity matrix. We may diagonalize A over $\mathcal{O}_K$ as follows:

$$(\chi^{-1}(g))A(\chi(g))^\top = v\,\mathrm{diag}(\chi(D)), \tag{2.4}$$

where $\chi(D) = \sum_{g\in G} a_g \chi(g)$.

Viewing A as a matrix with entries in $\mathbb{Z}$, we use $S = \mathrm{diag}(d_1, d_2, \ldots, d_v)$ to denote the Smith normal form of A over $\mathbb{Z}$. Then there exist integral unimodular matrices P and Q such that $A = PSQ$. Therefore, we have

$$(\chi^{-1}(g))PSQ(\chi(g))^\top = v\,\mathrm{diag}(\chi(D)). \tag{2.5}$$

This shows that S and $\mathrm{diag}(\chi(D))$, viewed as matrices with entries in $\mathcal{O}_K$, are equivalent over $\mathcal{O}_K$. Noting that $\mathcal{O}_K$ is a principal ideal domain, we see that S and $\mathrm{diag}(\chi(D))$ have the same invariant factors up to unit multipliers (cf. [10, p. 184]). Since $\mathcal{O}_K$ is local, and K is unramified over $\mathbb{Q}_p$ as $p \nmid v$, each $\chi(D)$ can be written as the product of a power of p and a unit in $\mathcal{O}_K$. So if we arrange the elements on the diagonal of $\mathrm{diag}(\chi(D))$ in such a way that the $v_p(\chi(D))$ are nondecreasing, then $\mathrm{diag}(\chi(D))$ can serve as a Smith normal form of A over $\mathcal{O}_K$. Therefore the two lists $v_p(d_i)$ and $v_p(\chi(D))$ are exactly the same. Noting that $p \nmid v$, we have $v_{\mathfrak{p}}(\chi(D)) = v_p(\chi(D))$: the conclusion of the lemma follows. □

We now state the global version of Lemma 2.1.

Lemma 2.2. *Let G be an abelian group of order v, let p be a prime not dividing v, and let $\mathfrak{P}$ be a prime ideal in $\mathbb{Z}[\xi_v]$ lying above p, where ξ_v is a complex primitive vth root of unity. Let D be a (v,k,λ) difference set in G, and let α be a positive integer. Then the*

number of invariant factors of D which are not divisible by p^α is equal to the number of complex characters χ of G such that $\chi(D) \not\equiv 0 \pmod{\mathfrak{P}^\alpha}$.

Proof. Let A be the matrix defined in the proof of Lemma 2.1. We may use A as the incidence matrix of the design $(G, \{Dg \mid g \in G\})$ developed from D. Similarly, let $(\chi^{-1}(g))$ be a matrix whose rows are labeled by the v complex characters χ and whose columns are labeled by the v group elements g, so that the entry in row χ and column g is $\chi^{-1}(g)$. Then we may diagonalize A over $\mathbb{Q}(\xi_v)$ as follows:

$$(\chi^{-1}(g))A(\chi(g))^\top = v\,\mathrm{diag}(\chi(D)), \tag{2.6}$$

where $\chi(D) = \sum_{g \in D} \chi(g)$.

Viewing A as a matrix with entries in $\mathbb{Z}$, we use $S = \mathrm{diag}(d_1, d_2, \ldots, d_v)$ to denote the Smith normal form of A over $\mathbb{Z}$. Then there exist integral unimodular matrices P and Q such that $A = PSQ$. Therefore, we have

$$(\chi^{-1}(g))PSQ(\chi(g))^\top = v\,\mathrm{diag}(\chi(D)). \tag{2.7}$$

Let $L = \mathbb{Q}(\xi_v)$, and let $L_\mathfrak{P}$ be the completion of L at $\mathfrak{P}$. $L_\mathfrak{P}$ is an extension field of $\mathbb{Q}_p$, and we may view L as embedded in $L_\mathfrak{P}$. Since $\gcd(p, v) = 1$, L is unramified over $\mathbb{Q}$, hence $L_\mathfrak{P}$ is unramified over $\mathbb{Q}_p$. Let $\mathcal{O}_\mathfrak{P}$ be the valuation ring in $L_\mathfrak{P}$, and let $\mathfrak{p}$ be the unique prime ideal in $\mathcal{O}_\mathfrak{P}$ lying above p. Then for every $a \in L_\mathfrak{P}$, we have

$$v_\mathfrak{P}(a) = v_\mathfrak{p}(a) \tag{2.8}$$

Now view all matrices in (2.7) as matrices with entries in $\mathcal{O}_\mathfrak{P}$. We see that S and $\mathrm{diag}(\chi(D))$ are equivalent over $\mathcal{O}_\mathfrak{P}$. Noting that $\mathcal{O}_\mathfrak{P}$ is a principal ideal domain, we see that S and $\mathrm{diag}(\chi(D))$ have the same invariant factors up to unit multipliers (cf. [10, p. 184]). Since $\mathcal{O}_\mathfrak{P}$ is local and $L_\mathfrak{P}$ is unramified over $\mathbb{Q}_p$, each $\chi(D)$ can be written as the product of a power of p and a unit in $\mathcal{O}_\mathfrak{P}$. So if we arrange the elements on the diagonal of $\mathrm{diag}(\chi(D))$ appropriately so that the $v_p(\chi(D))$ are nondecreasing, then $\mathrm{diag}(\chi(D))$ can serve as a Smith normal form of A over $\mathcal{O}_\mathfrak{P}$. Hence the two lists $v_p(d_i)$ and $v_p(\chi(D))$ are exactly the same. Note that by (2.8), we have $v_\mathfrak{P}(\chi(D)) = v_\mathfrak{p}(\chi(D))$, and $v_\mathfrak{p}(\chi(D)) = v_p(\chi(D))$. The conclusion of the lemma follows. □

Remark. Lemma 2.2 generalizes a result of MacWilliams and Mann [15], which asserts that the GF(p)-rank of A is equal to the number of complex characters χ such that $\chi(D) \not\equiv 0 \pmod{\mathfrak{P}}$.

Finally, we note that if $\mathscr{D}$ is a $((q^m - 1)/(q-1), q^{m-1}, q^{m-2}(q-1))$ symmetric design, where $q = p^s$, p is prime, and A is the incidence matrix of $\mathscr{D}$, then

$$\det(A) = q^{(m-2)(v-1)/2+(m-1)}, \tag{2.9}$$

where $v = (q^m - 1)/(q-1)$. Therefore the invariant factors of A are all powers of p. The number of invariant factors of A which are 1 is exactly the rank of A over $\mathbb{Z}/p\mathbb{Z}$, which is usually called *the p-rank of* $\mathscr{D}$. In the next section, we will be interested in not only the number of ones among the invariant factors of A, but also the number of p's among the invariant factors of A.

3. The invariant factors of the HKM and Lin difference sets

In this section we will show that the Lin difference sets and the HKM difference sets are in general inequivalent when they are comparable. Note that both these difference sets have parameters $((q^m-1)/(q-1), q^{m-1}, q^{m-2}(q-1))$, $q=3^e$, so by the discussion at the end of the previous section, the invariant factors of these difference sets are all powers of 3. Although the numbers of ones among the invariant factors of these two difference sets are the same in the case $e=1$ (cf. [6,16]), we will show that the numbers of 3's are different.

Let $q=3^e$, $e\geqslant 1$, let $m=3k$ and $d=q^{2k}-q^k+1$ (this is the HKM case); or let $q=3^e$, $e=1$, $m=2n+1$ and $d=2\cdot 3^n+1$ (this is the Lin case). Let $\rho: \mathbb{F}_{q^m}^* \to \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ be the natural epimorphism, and let

$$D=\{\rho(x) \mid x\in\mathbb{F}_{q^m} \text{ and } \mathrm{Tr}_{q^m/q}(x+x^d)=1\}$$

be the difference sets defined in Section 1. We first give explicit expressions for the character sums $\chi(D)$, where χ is any complex character of $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$. This was done in [6]; we include these computations here for the convenience of the reader.

Let L be a complete system of coset representatives of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^m}^*$, and let $L_0=\{x\in L \mid \mathrm{Tr}_{q^m/q}(x+x^d)=0\}$. If $x\in L$ and $\mathrm{Tr}_{q^m/q}(x+x^d)=a\neq 0$, then we may replace x by x/a, and

$$\mathrm{Tr}_{q^m/q}\left(\frac{x}{a}+\left(\frac{x}{a}\right)^d\right)=\mathrm{Tr}_{q^{3k}/q}(x+x^d)/a=1.$$

Therefore we may choose L such that $L=L_0\cup L_1$, where $L_1=\{x\in L \mid \mathrm{Tr}_{q^m/q}(x+x^d)=1\}$. It is then easy to see that

$$L_1=\{x\in\mathbb{F}_{q^m} \mid \mathrm{Tr}_{q^m/q}(x+x^d)=1\} \quad \text{and} \quad D=\rho(L_1).$$

Given any multiplicative character χ of $\mathbb{F}_{q^m}$, we define the sum

$$S_d(\chi)=\sum_{x\in\mathbb{F}_{q^m}^*}\chi(x)\xi_3^{\mathrm{Tr}_{q^m/3}(x+x^d)}. \tag{3.1}$$

Writing $x=ay$, with $a\in\mathbb{F}_q^*$ and $y\in L$, we have

$$\begin{aligned} S_d(\chi)&=\sum_{a\in\mathbb{F}_q^*}\chi(a)\sum_{y\in L}\chi(y)\xi_3^{\mathrm{Tr}_{q/3}(a\mathrm{Tr}_{q^m/q}(y+y^d))}\\ &=\sum_{y\in L_0}\chi(y)\sum_{a\in\mathbb{F}_q^*}\chi(a)+\sum_{y\in L_1}\chi(y)\sum_{a\in\mathbb{F}_q^*}\chi(a)\xi_3^{\mathrm{Tr}_{q/3}(a)}. \end{aligned}$$

If $\chi=1$, then $S_d(1)=(q-1)|L_0|-|L_1|=q^m-1-q|L_1|$.

If $\chi\neq 1$, but $\chi|_{\mathbb{F}_q^*}=1$, then $S_d(\chi)=-q\chi(L_1)$.

If $\chi\neq 1$, and $\chi|_{\mathbb{F}_q^*}\neq 1$, then $S_d(\chi)=\chi(L_1)\cdot g_1(\chi_1)$, where χ_1 is the restriction of χ to $\mathbb{F}_q^*$, and $g_1(\chi_1)$ is the Gauss sum over the finite field $\mathbb{F}_q$ with respect to χ_1.

In summary, if χ is a nontrivial multiplicative character of $\mathbb{F}_{q^m}$, then

$$\chi(L_1) = \begin{cases} -\frac{1}{q} S_d(\chi) & \text{if } \chi|_{\mathbb{F}_q^*} = 1, \\ \frac{S_d(\chi)}{g_1(\chi_1)} & \text{if } \chi|_{\mathbb{F}_q^*} \neq 1. \end{cases} \tag{3.2}$$

For $\mathfrak{P}$ a prime ideal in $\mathbb{Z}[\xi_{q^m-1}]$ lying over 3, let $\omega_{\mathfrak{P}}$ be the Teichmüller character on $\mathbb{F}_{q^m}$. Then any nontrivial character of $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ takes the form $\omega_{\mathfrak{P}}^{-a}$, $0<a<(q^m-1)$ with $(q-1)|a$. By (3.2), for any a, $0<a<(q^m-1)$ and $(q-1)|a$, we have

$$\omega_{\mathfrak{P}}^{-a}(D) = \omega_{\mathfrak{P}}^{-a}(L_1) = -\frac{1}{q} S_d(\omega_{\mathfrak{P}}^{-a}). \tag{3.3}$$

Let $\tilde{\mathfrak{P}}$ be the prime of $\mathbb{Z}[\xi_{q^m-1}, \xi_3]$ lying above $\mathfrak{P}$, and let

$$t_d(a) = v_{\tilde{\mathfrak{P}}}(S_d(\omega_{\mathfrak{P}}^{-a})) \tag{3.4}$$

be the $\tilde{\mathfrak{P}}$-adic valuation of $S_d(\omega_{\mathfrak{P}}^{-a})$.

Lemma 3.1. *With the above notation, for any nonnegative integer $\alpha \leqslant m-2$, the number of invariant factors of D which are 3^α is*

$$|\{a \mid 0<a<(q^m-1),\ (q-1)|a,\ t_d(a) = 2e+2\alpha\}|.$$

Proof. By Lemma 2.2, the number of invariant factors of D which are 3^α is equal to the number of $\omega_{\mathfrak{P}}^{-a}$, $0<a<(q^m-1)$ and $(q-1)|a$, such that $\mathfrak{P}^\alpha || \omega_{\mathfrak{P}}^{-a}(D)$. As ideals in $\mathbb{Z}[\xi_{q^m-1}, \xi_3]$, $\mathfrak{P} = \tilde{\mathfrak{P}}^2$. Hence the number of invariant factors of D which are 3^α is equal to the number of $\omega_{\mathfrak{P}}^{-a}$, $0<a<(q^m-1)$ and $(q-1)|a$, such that $\tilde{\mathfrak{P}}^{2\alpha} || \omega_{\mathfrak{P}}^{-a}(D)$.

To simplify notation, we will usually drop the index in $\omega_{\mathfrak{P}}$ if there is no confusion. By (3.3), we have $\omega^{-a}(D) = -\frac{1}{3^e} S_d(\omega^{-a})$. By definition, we have

$$v_{\tilde{\mathfrak{P}}}(S_d(\omega^{-a})) = t_d(a).$$

Also it is clear that $v_{\tilde{\mathfrak{P}}}(3^e) = 2e$. Therefore, the number of a, $0<a<(q^m-1)$, $(q-1)|a$ such that $\tilde{\mathfrak{P}}^{2\alpha} || \omega^{-a}(D)$ is equal to the cardinality of the set

$$\mathcal{T}_\alpha = \{a \mid 0<a<(q^m-1),\ (q-1)|a,\ t_d(a) = 2e+2\alpha\}. \tag{3.5}$$

We will denote this cardinality by T_α, and we have shown that the number of invariant factors of D which are 3^α is equal to T_α. This completes the proof. □

In order to compute explicitly the number of invariant factors of D which are 3^α, we need to compute $t_d(a)$ first. By the definition of Gauss sums, we have

$$g(\omega^b) = \sum_{x \in \mathbb{F}_{q^m}^*} \omega^b(x) \zeta_3^{\mathrm{Tr}_{q^m/3}(x)}.$$

Using Fourier inversion, we find that

$$\xi_3^{\mathrm{Tr}_{q^m/3}(x^d)} = \frac{1}{q^m-1}\sum_{b=0}^{q^m-2} g(\omega^{-b})\omega^b(x^d).$$

Therefore

$$\begin{aligned} S_d(\omega^{-a}) &= \frac{1}{q^m-1}\sum_{x\in\mathbb{F}_{q^m}^*} \omega^{-a}(x)\xi_3^{\mathrm{Tr}_{q^m/3}(x)}\sum_{b=0}^{q^m-2} g(\omega^{-b})\omega^{bd}(x) \\ &= \frac{1}{q^m-1}\sum_{b=0}^{q^m-2} g(\omega^{-b})g(\omega^{bd-a}). \end{aligned}$$

For any integer x not divisible by q^m-1, we as usual use $s(x)$ to denote the 3-adic weight of $x \pmod{q^m-1}$. In addition, if $x \equiv 0 \pmod{q^m-1}$, we set $s(x)=0$. With this convention, using Stickelberger's theorem on the prime ideal decomposition of Gauss sums [9, p. 212], we find that

$$t_d(a) \geqslant \min_{0\leqslant b\leqslant q^m-2}\{s(b)+s(a-bd)\}. \tag{3.6}$$

Moreover, if the above minimum is attained at *exactly one* value of b in the range $[0, q^m-2]$, then

$$t_d(a) = \min_{0\leqslant b\leqslant q^m-2}\{s(b)+s(a-bd)\}.$$

In general, the function $t_d(a)$ is hard to control, hence it is difficult to compute explicitly the cardinality of $\mathscr{T}_\alpha$ (see (3.5) for definition). In [6], we computed T_0 in the case $q=3$. In the following, we will assume that $q=3$, i.e., $e=1$, and find explicit formulas for the cardinality T_1 of

$$\mathscr{T}_1 = \{a \mid 0<a<3^m-1, 2|a, t_d(a)=4\},$$

for both d given at the beginning of this section.

When calculating the 3-ranks of the HKM and Lin difference sets in [6] in the case $q=3$, that is computing the number of even a, $0<a<3^m-1$, for which $t_d(a)=2$, we first list all a, $0<a<3^m-1$, such that $\min_{0\leqslant b\leqslant 3^m-2}\{s(b)+s(a-bd)\}=2$; in both the HKM and Lin cases, there are exactly two values of a, up to cyclic shift, for which $s(b)+s(a-bd)=2$ at more than one value of b when $m>3$. (For all other a in the list, there is a unique b in the range $[0, 3^m-2]$ such that $s(b)+s(a-bd)=2$: thus $t_d(a)=2$.) For these two "exceptional" values of a, we had to do more detailed analysis to decide whether $t_d(a)=2$ or $t_d(a)>2$. In the former case, we count the a towards the 3-rank, and in the latter case we do not. The final conclusion is that both HKM and Lin difference sets have 3-rank $2m^2-2m$ when $m>3$ (see [6,16]).

Now if we want to count the number of invariant factors which are 3 for the HKM and Lin difference sets, we need to compute the number T_1 of even a, $0<a<3^m-1$, for which $t_d(a)=4$. Again we need to pay special attention to those a, for which $s(b)+s(a-bd)=4$ at more than one value of b (we again call these a "exceptional"). Unfortunately, the list of such a's already becomes awkwardly large. Instead of analyzing each "exceptional" a individually, we argue that, except for small m, T_1 is a fourth degree polynomial in m with leading term $\frac{2}{3}m^4$, or differs from it by exactly m. Then we use a computer to calculate T_1 for various m to pin down the remaining coefficients of the fourth degree polynomial.

Lemma 3.2. *With the notation above, for $m>7$ in the Lin case, and for $m>9$ in the HKM case, the number of even values of a for which $\min_{0\leqslant b\leqslant 3^m-2}\{s(b)+s(a-bd)\}=4$ is a fourth degree polynomial in m. Furthermore, the leading term is $\frac{2}{3}m^4$.*

Proof. First, we count the total number of pairs (a,b), $0<a\leqslant 3^m-2$, $0\leqslant b\leqslant 3^m-2$, for which $s(b)+s(a-bd)=4$. If $s(b)=4$ and $s(a-bd)=0$, then $a=bd$ and b has 3-adic representation as one of the following: four 1's and the rest 0's; two 1's, one 2, and the rest 0's; or two 2's and the rest 0's. Similarly if $s(b)=3$ then b is either three 1's and the rest 0's; or one 1, one 2, and the rest 0's; while $a=bd+3^i$ for some i between 0 and $m-1$. If $s(b)=2$ then b has either two 1's and the rest 0's; or one 2 and the rest 0's; while $a-bd$ also has one of those forms. The cases $s(b)=1$ and 0 mirror the cases $s(b)=3$ and 4.

Since $s(a-bd)=4-s(b)$, we can write $a=bd+x$, where $s(x)=4-s(b)$. So we may think of a as represented by the sum of 4 terms, each either a shift of d, or a shift of 1. Here if the 3-adic representation of b or $a-bd$ has a digit 2, then the corresponding copy of d or of 1 is viewed as 3^id+3^id, or 3^i+3^i (i.e., a sum of two terms). Observing that since d is odd $a=bd+x$ is necessarily even if $s(b)+s(x)=4$, we find from the discussion in the previous paragraph that the total number of pairs (a,b) for which $s(b)+s(a-bd)=4$ and a is even is

$$2\binom{m}{4}+2\binom{m}{2}(m-2)+2\binom{m}{2}+2\binom{m}{3}m+2m^2(m-1)$$
$$+\left(\binom{m}{2}+m\right)^2=\frac{2}{3}m^4+2m^3-\frac{13}{6}m^2+\frac{1}{2}m. \tag{3.7}$$

In order to prove the assertion of the lemma we need to subtract from this polynomial the number of pairs (a,b) which are redundant for any value of a, as well as the number of those a's included here but which can also be represented as $bd+x$, with $s(b)+s(x)=2$.

For convenience we will sometimes think of a and d as written using the digits 0,1, and -1 (mostly in the HKM case). Thus, if a has a 2 in it, replace it with -1 and carry 1 to the next higher place. Similarly, -2 gets replaced by 1 and -1 gets carried.

With this convention, it is easy to see that the possible number of nonzero digits in a does not grow as m grows.

We now classify the above a's depending on how the digits of the four terms (each term a shift of 1 or of d) combine when added. If two a's are in the same class, then the numbers of shifts of d (resp. the numbers of shifts of 1) in the sums which produce the two a's are the same. Also there should be a correspondence between shifts of d in the two sums, and between shifts of 1 in the two sums, with the following property: if some of the nonzero digits happen to fall in one column in the sum for one a, the corresponding digits do likewise in the sum for the other a. Furthermore, any carry digits which also coincide with nonzero digits have the same property. Note that some of the addends have freedom to shift with respect to each other within the same class of a, while others do not. For instance, the following sums would produce a's in the same class:

$$\begin{array}{cccccccccc}
0&0&0&2&0&0&0&1&0\\
0&2&0&0&0&1&0&0&0\\
1\\
1\\
\hline
2&2&0&2&0&1&0&1&0
\end{array}
\qquad
\begin{array}{cccccccccc}
0&0&0&2&0&0&0&1&0\\
1&0&0&0&0&2&0&0&0\\
&&&&1\\
&&&&1\\
\hline
1&0&0&2&2&2&0&1&0
\end{array}$$

but the following would represent two other classes:

$$\begin{array}{cccccccccc}
0&0&0&0&2&0&0&0&1\\
0&0&0&0&2&0&0&0&1\\
&&&1\\
&&&1\\
\hline
0&0&1&0&1&0&0&0&2
\end{array}
\qquad
\begin{array}{cccccccccc}
0&0&0&0&2&0&0&0&1\\
0&0&2&0&0&0&1&0&0\\
&&1\\
&&&1\\
\hline
0&1&2&1&2&0&1&0&1
\end{array}$$

In the first example the addends have three degrees of freedom to shift, while in the last example there are four degrees of freedom and in the middle one there is only one degree of freedom. Thus, in the first example, there are $m=9$ choices of shift for the first copy of d. There are only $m-3$ choices for the second copy of d, $m-4$ choices for the first copy of 1, and the second copy of 1 is determined by the first. Here we ignore the possibility that other values of b might be associated with some of these a's. It is also clear that the pattern remains the same if we increase m by inserting extra pairs of columns of 0's.

Now we continue the definition of classes where a given value of a is associated with more than one value of b. The following sums give an example of such a situation:

$$\begin{array}{cccccccccc}
0&0&0&0&2&0&0&0&1\\
0&0&0&0&2&0&0&0&1\\
1\\
1\\
\hline
2&0&0&1&1&0&0&0&2
\end{array}
=
\begin{array}{cccccccccc}
2&0&0&0&1&0&0&0&0\\
&&&&1\\
&&&&&&&&1\\
\hline
2&0&0&1&1&0&0&0&2
\end{array}
=
\begin{array}{cccccccccc}
0&0&0&1&0&0&0&0&2\\
1\\
1\\
&&&&1\\
\hline
2&0&0&1&1&0&0&0&2
\end{array}$$

Here, two values of a_1 and a_2 will be considered to be in the same class only if the pairs (a_1, b_{1i}) and (a_2, b_{2i}) are in one-to-one correspondence such that the sum $a_1 = b_{1i}d + x_{1i}$ is a shift of $a_2 = b_{2i}d + x_{2i}$ for each i.

Each class of a has some number of degrees of freedom. The maximum is 4, in the case that the nonzero digits of the addends are totally disjoint. If two different sums $b_1d + x_1$ and $b_2d + x_2$ are the same, say both equal a, the degree of freedom of that class of a is at most 3. Otherwise, the nonzero digits of the addends are totally disjoint; hence the positions of the 2's in a, in the Lin case, or of (-1)'s in a, in the HKM case, reflect the positions of copies of d in the sum. Thus $b_1 = b_2$, contradicting our assumption that there are two different sums producing the same a.

In general, for each degree of freedom, we can pick any shift from 0 to $m-1$, except for a fixed number of possibilities that cause sectors of a to overlap. In cases such as

$$\begin{array}{cccccccccc} 0 & 0 & & 1 & 0 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & & 1 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 & 0 & & 1 & 0 & 0 & 1 \\ 1 & & & & & & & & & \\ \hline 1 & 0 & & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{array}$$

shifts of the three copies of d have a period of $m/3$. Thus, the size of this class of a (ignoring other values of b) would be $(m/3)(m-3)$. So each class of a's has cardinality of a polynomial of degree equal to the number of degrees of freedom and each a in a class has the same number of associated b's. In order to prove the assertion of the lemma, we subtract from (3.7) a polynomial of degree at most three for each class of a for which the number of associated b is more than one. We also have to subtract the number of a's which we have counted but for which $\min_{0 \leqslant b \leqslant q^m-2} \{s(b) + s(a - bd)\} = 2$. These cases have at most two degrees of freedom, so we subtract from (3.7) another polynomial of degree at most two.

Finally, the following sums for $m = 7$ (in the Lin case) and $m = 9$ (in the HKM case) represent the only classes of a for those m for which a sequence of carries continues from one nonzero digit of d to the next:

$$\begin{array}{cccccccccc} 0 & 0 & 0 & 2 & 0 & 0 & 1 & = & d \\ 0 & 0 & 2 & 0 & 0 & 1 & 0 & = & 3d \\ 0 & 2 & 0 & 0 & 1 & 0 & 0 & = & 9d \\ 2 & 0 & 0 & 1 & 0 & 0 & 0 & = & 27d \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 2 & = & 3^2 + 3 + 2 \end{array} \tag{3.8}$$

$$
\begin{array}{ccccccccc|cc}
0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 1 & = & d \\
0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 1 & = & d \\
0 & 1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & = & 3d \\
1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & = & 9d \\
\hline
-1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & & \\
 & & & & & & & & & & \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & -1 & = & 3^6 d \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & = & 3^7 d \\
1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & = & 3^8 d \\
 & & & & & 1 & & & & = & 3^3 \\
\hline
-1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & &
\end{array}
\tag{3.9}
$$

In each of these two cases we have two values of b associated with the same a, while for all higher m, we get two different values of a for the corresponding sums. That is, these sums are special, and would not happen if the number m of digits is large. So for $m>7$ in the Lin case, and for $m>9$ in the HKM case, the number of even a such that $\min_{0\leqslant b\leqslant 3^m-2}\{s(b)+s(a-bd)\}=4$ is a fourth degree polynomial in m with leading term $\frac{2}{3}m^4$. □

We proceed to compute $T_1=|\mathscr{T}_1|=|\{a\mid 0<a<3^m-1, 2|a, t_d(a)=4\}|$. By (3.6), we see that

$$T_1=|\mathscr{A}\backslash\mathscr{B}|+|\mathscr{C}|,$$

where

$$\mathscr{A}=\left\{a\mid 0<a<3^m-1, 2|a, \min_{0\leqslant b\leqslant 3^m-2}\{s(b)+s(a-bd)\}=4\right\},$$

$$\mathscr{B}=\left\{a\mid 0<a<3^m-1, 2|a, \min_{0\leqslant b\leqslant 3^m-2}\{s(b)+s(a-bd)\}=4, \text{ and } t_d(a)>4\right\},$$

$$\mathscr{C}=\left\{a\mid 0<a<3^m-1, 2|a, \min_{0\leqslant b\leqslant 3^m-2}\{s(b)+s(a-bd)\}=2, \text{ and } t_d(a)=4\right\}.$$

By Lemma 3.2, for $m>7$ in the Lin case, and for $m>9$ in the HKM case, $|\mathscr{A}|$ is a polynomial in m of degree 4 with leading term $\frac{2}{3}m^4$. We will show that $|\mathscr{B}|$ is a polynomial in m of degree at most 3. In order to compute $|\mathscr{B}|$, we have to distinguish those classes of a in $\mathscr{A}$ for which $t_d(a)=4$, and those for which $t_d(a)>4$, that is, decide whether

$$\tilde{\mathfrak{P}}^4||\frac{1}{3^m-1}\sum_{b=0}^{3^m-2} g(\omega^{-b})g(\omega^{bd-a})$$

or

$$\tilde{\mathfrak{P}}^5 \mid \frac{1}{3^m-1}\sum_{b=0}^{3^m-2} g(\omega^{-b})g(\omega^{bd-a}).$$

The distinction can be made with the help of Stickelberger's congruence for Gauss sums as stated in the following theorem.

Theorem 3.3 (Lang [13, p. 7]). *Let r be an integer with $0 \leqslant r < q-1 = p^m - 1$ and with p-adic expansion*

$$r = r_0 + r_1 p + \cdots + r_{m-1}p^{m-1}$$

with $0 \leqslant r_i \leqslant p-1$. Define

$$\gamma(r) = r_0! r_1! \cdots r_{m-1}!$$

Then with $s(r)$ and ω as above we have the congruence

$$\frac{g(\omega^{-r})}{(\xi_p - 1)^{s(r)}} \equiv \frac{-1}{\gamma(r)} \pmod{\tilde{\mathfrak{P}}}.$$

Lemma 3.4. *For $m>7$ in the Lin case, and for $m>9$ in the HKM case, $|\mathscr{B}|$ is a polynomial in m of degree at most 3.*

Proof. Given an integer r, $0 \leqslant r < 3^m - 1$, since $\tilde{\mathfrak{P}} \mid 3$, we have $\gamma(r) \equiv 1$ or $\gamma(r) \equiv -1 \pmod{\tilde{\mathfrak{P}}}$, depending on whether the 3-adic representation of r has an even number of twos or an odd number of twos. Given $a \in \mathscr{A}$, applying Stickelberger's congruence to those terms in the sum $\sum_{b=0}^{3^m-2} g(\omega^{-b})g(\omega^{bd-a})$ for which $s(b) + s(a-bd) = 4$ we get

$$\frac{g(\omega^{-b})g(\omega^{bd-a})}{(\xi_3 - 1)^4} \equiv \gamma(b)\gamma(a-bd) \pmod{\tilde{\mathfrak{P}}}.$$

Summing over these b's, noting that $\tilde{\mathfrak{P}} \| (\xi_3 - 1)$, we see that $a \in \mathscr{B}$ iff

$$\sum_{s(b)+s(a-bd)=4} \gamma(b)\gamma(a-bd) \equiv 0 \pmod 3.$$

For example in (3.8), $m = 7$, for $a = 3^2 + 3 + 2$, we have two b's such that $s(b) + s(a-bd) = 4$. The first is $b = 1111$ (and $a - bd = 0$). The second is $b = 0$ (and $a - bd = 112$). Since $\gamma(1111)\gamma(0) + \gamma(0)\gamma(112) = 1 \cdot 1 + 1 \cdot (-1) = 0$, we conclude that this a is in $\mathscr{B}$. Similarly, in (3.9), $m = 9$, for $a = -3 - 3^2 - 3^3 - \cdots - 3^8$, we also have two b's such that $s(b) + s(a-bd) = 4$, namely, $b = 112$ (and $a - bd = 0$), or $b = 111$ (and $a - bd = 1000$). Again the sum $\gamma(112)\gamma(0) + \gamma(111)\gamma(1000)$ is 0, and so this a is in $\mathscr{B}$.

We observe that if an $a \in \mathscr{A}$ is in $\mathscr{B}$, then the whole class to which a belongs is in $\mathscr{B}$. The reason is given as follows. By definition, within each class of a's, the set of b's for which $s(b) + s(a-bd) = 4$ for one a have 3-adic representations which are

permutations of the 3-adic representations of the b's corresponding to any other a in that class, and since the 3-adic representations of the corresponding values of $a-bd$ are also permutations of each other, the set of values of $\gamma(b)\gamma(a-bd)$ are the same for each a in a class, therefore for two a's in the same class, the corresponding $t_d(a)$'s are either both equal to 4 or both greater than 4.

Finally, note that if an element $a\in\mathscr{A}$ is in $\mathscr{B}$ then there are more than one b such that $s(b)+s(a-bd)=4$. By the discussion in the proof of Lemma 3.2, the size of these classes of a is a polynomial in m of degree at most 3 when $m>7$ in the Lin case, and $m>9$ in the HKM case. Hence the conclusion of the lemma follows. □

We were not able to determine $\mathscr{C}$ completely. However from our work in [6], we know that when $m>3$, in both the Lin and HKM cases, there is only one value of a (and its cyclic shifts) satisfying $\min_{0\leqslant b\leqslant q^m-2}\{s(b)+s(a-bd)\}=2$ but $t_d(a)>2$. Hence $|\mathscr{C}|=0$ or m. The a's which are possibly in $\mathscr{C}$ are given below. In the Lin case we have

$$\begin{array}{cccccccccc} 0&0&\cdots&0&2&0&\cdots&1&=&d\\ 0&0&\cdots&0&2&0&\cdots&1&=&d\\ \hline 0&0&\cdots&1&1&0&\cdots&2&=&a \end{array} \qquad \begin{array}{cccccccccc} 0&0&\cdots&1&0&0&\cdots&2&=&3^{\frac{m+1}{2}}d\\ &&\cdots&&1&&\cdots&&=&3^{\frac{m-1}{2}}\\ \hline 0&0&\cdots&1&1&0&\cdots&2&=&a \end{array} \tag{3.10}$$

while in the HKM case we have

$$\begin{array}{ccccccccccccc} 0&\cdots&0&1&0&\cdots&0&-1&0&\cdots&0&1&=&d\\ 0&\cdots&0&-1&0&\cdots&0&1&0&\cdots&0&1&=&3^{m/3}d\\ \hline 0&\cdots&0&0&0&\cdots&0&0&0&\cdots&0&2&=&a \end{array} \tag{3.11}$$

Using MAPLE to compute $|\mathscr{A}\backslash\mathscr{B}|$ up to $m=27$, we get the following theorem.

Theorem 3.5. *Let $q=3$. The number of 3's in the Smith normal form of the Lin difference sets when $m>7$ is*

$$\tfrac{2}{3}m^4-4m^3-\tfrac{14}{3}m^2+39m+\delta(m)m.$$

The number of 3's in the Smith normal form of the HKM difference sets when $m>9$ is

$$\tfrac{2}{3}m^4-4m^3-\tfrac{28}{3}m^2+62m+\varepsilon(m)m.$$

The values of $\delta(m)$ and $\varepsilon(m)$ are 0 or 1.

Based on numerical evidence, we conjecture that δ and ε above are always 1.

By direct calculations (i.e., not using Gauss sums), the Smith normal form of the Lin difference set with $m=9$ is

$$1^{144}3^{1440}9^{1572}27^{1764}81^{1764}243^{1572}729^{1440}2187^{144}6561^{1},$$

where for example, 3^{1440} means the number of invariant factors of the Lin difference set which are 3 is 1440. The Smith normal form of the HKM difference set with

$m = 9$ is

$$1^{144}3^{1251}9^{1842}27^{1683}81^{1683}243^{1842}729^{1251}2187^{144}6561^{1}.$$

These computations were done by Saunders [18].

Since the two "almost" polynomial functions in Theorem 3.5 are never equal, and since the Smith normal forms of the Lin and HKM difference sets are also different when $m = 9$, we have the following conclusion:

Theorem 3.6. *Let m be an odd multiple of 3. The Lin and HKM difference sets with parameters $(\frac{3^m-1}{2}, 3^{m-1}, 2\cdot 3^{m-2})$ are inequivalent when $m>3$, and the associated designs are nonisomorphic when $m>3$.*

The research of this note prompts the following question: If two cyclic difference sets with classical parameters have the same Smith normal form, are the associated designs necessarily isomorphic?

We note that certainly there are examples of nonisomorphic symmetric designs with classical parameters having the same Smith normal form. Projective planes of order 9 provide such examples. It is known [3] that the Smith normal form of a projective plane of order p^2, p prime, is

$$1^r p^{(p^4+p^2-2r+2)}(p^2)^{(r-2)}((p^2+1)p^2)^1,$$

where the exponents indicate the multiplicities of the invariant factors and r is the p-rank of the plane. That is, the p-rank of the plane determines the Smith normal form of the plane. There are four projective planes of order 9. The desarguesian one has 3-rank 37, while the other three all have 3-rank 41 (cf. [17]), so the three non-desarguesian projective planes have the same Smith normal form, yet they are nonisomorphic.

So far, we do not know any examples of difference sets with classical parameters which provide a negative answer to the question above. Difference set designs are special; it is of interest to investigate the above problem.

Acknowledgments

We thank W.K. Chan for suggesting the local approach in the current proofs of Lemmas 2.1 and 2.2. We also thank J.F. Dillon and B.D. Saunders for their comments and help. The research of the second author was partially supported by NSA grant MDA 904-01-1-0036.

References

[1] K.T. Arasu, private communication, July, 2001.

[2] K.T. Arasu, K. Player, A family of cyclic difference sets with Singer parameters in characteristic 3, Des. Codes Cryptogr., to appear.

[3] E.F. Assmus Jr., Applications of algebraic coding theory to finite geometric problems, in: N.L. Johnson, M.J. Kallaher, C.T. Long (Eds.), Finite Geometries: Proceedings of a conference in honor of T.G. Ostrom, Lecture Notes in Pure and Applied Mathematics, Vol. 82, Dekker, New York, Pullman Washington, 1983, pp. 23–32.
[4] T. Beth, D. Jungnickel, H. Lenz, Design Theory, Vol. 1, 2nd Edition, Cambridge University Press, Cambridge, 1999.
[5] S.C. Black, R.J. List, One certain abelian groups associated with finite projective geometries, Geom. Dedicata 33 (1989) 13–19.
[6] D.B. Chandler, Q. Xiang, Cyclic relative difference sets and their p-ranks, Des. Codes Cryptogr., to appear.
[7] R. Evans, H.D.L. Hollmann, C. Krattenthaler, Q. Xiang, Gauss sums, Jacobi sums and p-ranks of difference sets, J. Combin. Theory Ser. A 87 (1999) 74–119.
[8] T. Helleseth, P.V. Kumar, H.M. Martinsen, A new family of ternary sequences with ideal two-level autocorrelation, Des. Codes Cryptogr. 23 (2001) 157–166.
[9] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, 2nd Edition, Springer, Berlin, 1990.
[10] N. Jacobson, Basic Algebra I, 2nd Edition, Freeman, San Francisco, 1985.
[11] E.S. Lander, Topics in algebraic coding theory, D.Phil. Thesis, Oxford University, 1980.
[12] E.S. Lander, Symmetric Designs: An Algebraic Approach, in: London Mathematical Society Lecture Note Series, Vol. 74, Cambridge University Press, Cambridge, 1983.
[13] S. Lang, Cyclotomic Fields, Springer, New York, 1978.
[14] R.A. Liebler, private communication, September 30, 2002.
[15] J. MacWilliams, H.B. Mann, On the p-rank of the design matrix of a difference set, Inform. Control 12 (1968) 474–488.
[16] J.-S. No, D.-J. Shin, T. Helleseth, On the p-ranks and characteristic polynomials of cyclic difference sets, preprint.
[17] H.E. Sachar, Error-correcting codes associated with finite projective planes, Ph.D. Thesis, Lehigh University, Bethlehem, PA, 1973.
[18] B.D. Saunders, personal communication.
[19] P. Sin, The elementary divisors of the incidence matrices of points and linear subspaces in $P^n(\mathbb{F}_p)$, J. Algebra 232 (2000) 76–85.
[20] Q. Xiang, Recent results on difference sets with classical parameters, in: A. Pott et al. (Eds.), Proceedings of the NATO ASI "Difference Sets, Sequences and their Correlation Properties", 1999, pp. 419–437.